Electronic Version
Stylesheet Version v1.1.1

Description

Reduction in unwanted e-mail (spam) through the use of portable unique utilization of public key infrastructure (PKI)

Summary of Invention

[0001] The primary weakness of email is its indiscriminate nature. It allows anyone to send a message to anyone else, without invitation or proof of identity.

[0002] All users of an enhanced electronic mail system will be identified via a unique public key.

[0003] Electronic mail servers and clients (including HTML web server based email clients) can be enhanced to automatically include this signature and sort incoming email based on the presence and validity of the signature.

[0004] This serves the purpose of unique identification of the source of every email. This identification is portable.

[0005] This also thwarts a common practice among the purveyors

of unwanted email, namely source spoofing.

Detailed Description

[0006] A PKI server (or servers) will be setup to serve as a third party certifier for each sender and receiver. Each end user will provide proof of identity to receive their first key, replace a lost key, or possibly to install on a new machine.

[0007] Keys will only be valid for a specific period of time. Assuming the decision to remove a user has not occurred due to misuse of the system, reported stolen keys, inactive account, request for closure, etc, a new key will be emailed to the end user.

[0008] When a new key is emailed, it will either be encrypted based on the old key and sent prior to the expiration of the old key, or it will be sent in a way that old key plus the email generate the new key.

[0009] An Email server (or servers) will be updated to only accept incoming mail with a valid signature or route to different folders based on the signature. Similarly, an email client can accept, reject, or route to folders based on signatures.

[0010] A signature is based on the key of the sender and the contents of the email and/or time. This results in a signature that is different each time, even though each time it is based on the same key. This prevents theft of a signa-

ture.

[0011] The portability of the unique key is beneficial in that one can send from any email address. For the system to be truly useful, members need to be able to reach each other no matter what email address is used. A system of email forwards will support this universal addressability. These email forwards can be maintained by the users or automatically, from the last email address used by the user.

[0012] The system of forwards does not prevent a central email account.

[0013] The use of digital signatures neither requires nor precludes the additional encryption.

[0014] This invention neither requires nor precludes other methods of controlling unwanted email, including but not limited to filters, domain authentication and email postage initiatives.

[0015] This system in no way prevents mass mailings. In some cases, such as discussion groups, news letters, and marketing for desired product, mass mailings are desired. No promise of conduct is required. Those that misuse the system can be dealt with by key expiration. No data related to number of recipients need be added to the email.

[0016] Usage of email forwarding system and any central system

can be monitored for usage patterns, including misuse.

[0017] In the event of sever misuse that can not wait for a key expiration, a "black list" can be supported. This would be a special message or messages sent to all connected servers and possibly end users to block all email from a specific user.